



(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:  
 27.02.2002 Bulletin 2002/09

(51) Int Cl.7: **H04L 29/06, H04Q 7/22,**  
**H04L 12/56**

(21) Application number: **01304277.5**

(22) Date of filing: **14.05.2001**

(84) Designated Contracting States:  
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU**  
**MC NL PT SE TR**  
 Designated Extension States:  
**AL LT LV MK RO SI**

(72) Inventor: **Xiaobao , Chen x**  
**Swindon, Wiltshire SN5 5DQ (GB)**

(74) Representative: **Sarup, David Alexander et al**  
**Lucent Technologies NS UK Limited, 5**  
**Mornington Road**  
**Woodford Green, Essex IG8 OTU (GB)**

(30) Priority: **21.08.2000 GB 0020582**

(71) Applicant: **LUCENT TECHNOLOGIES INC.**  
**Murray Hill, New Jersey 07974-0636 (US)**

(54) **Improved method of operating a mobile telecommunications network to provide route optimisation and quality of service**

(57) In a 3G telecom network, when a mobile wanders in a foreign network and a home agent (26) is allocated a Care of Address for the mobile, the home agent (26) also changes packet headers so that the destination address is the Care of Address, and there is a mobile node identifier field (50); the home agent maintains a mapping table of mobile nodes and mobile node identifiers.

Route optimization is therefore provided.

Quality of Service can be provided; when the mobile node sends a PATH message and a RSVP proxy server is built into the mobile node, the server changes the packet header source address to the mobile node Care of Address, to prevent misrouting of the RESV message to the home network.

**FIG. 4**

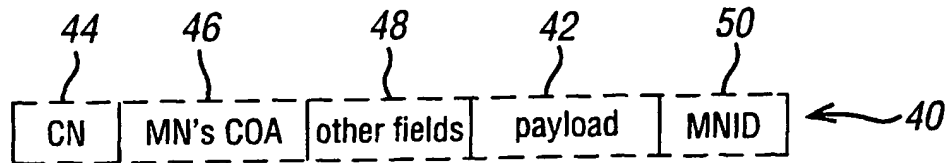


FIG. 5a

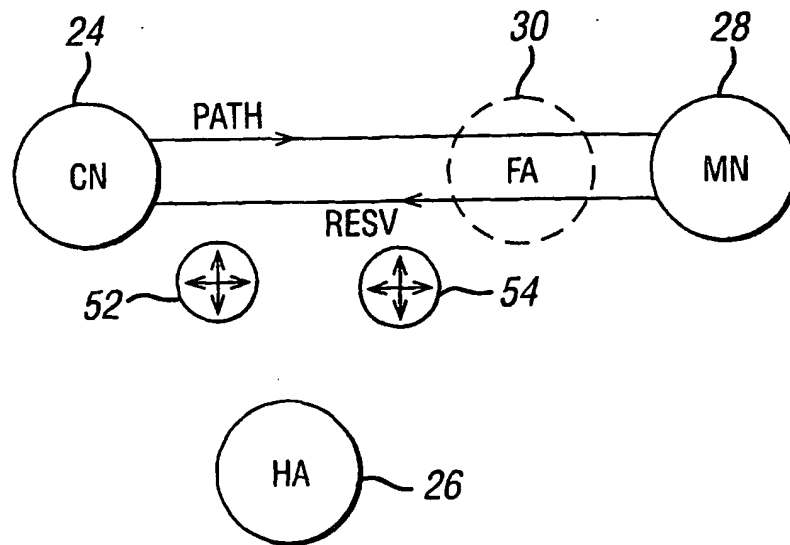
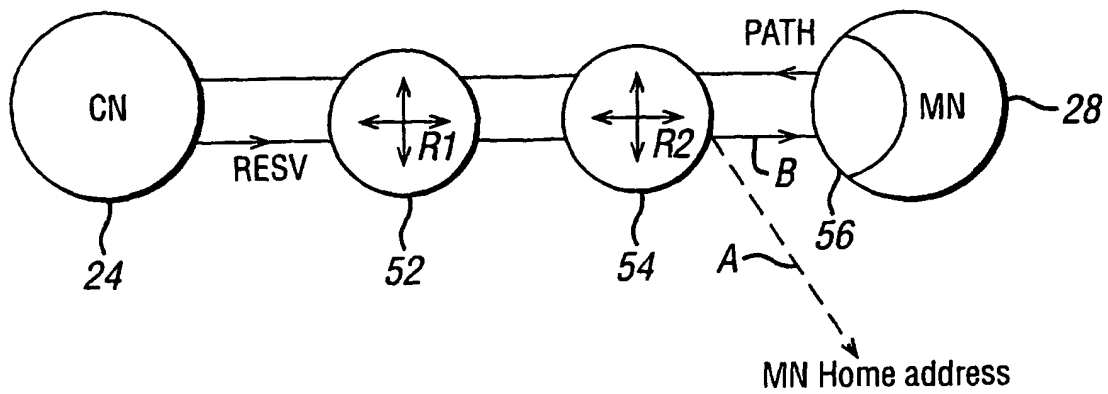


FIG. 5b



## Description

[0001] This invention relates to an improved method of operating a mobile telecommunications network, especially a third generation network, to provide route optimization and quality of service (QoS).

[0002] In third generation telecommunications networks such as GPRS (General Packet Radio Service) and EDGE (Enhanced Data-rate for GSM Evolution), when a mobile terminal moves into a foreign network, network connectivity is optionally maintained by the use of Mobile Internet Protocol (Mobile IP). In the home network, a Home Agent (HA) is set up which maintains the location information of the mobile by use of Binding Updates, i.e., registration of information sent to the HA by the mobile node.

[0003] Mobile IP has two working modes. The first is illustrated in Figure 1; a mobile terminal is currently attached as a Mobile Node (MN) 14 in a network different from its home network. The MN 14 is communicating with a Correspondent Node (CN) 12. A Home Agent 16 is set up in the home network by the CN 12, and a Foreign Agent (FA) 18 is set up in the foreign network. The FA 18 allocates a unique IP address for the visiting mobile, a Care of Address (COA) and this address is sent to the HA 16 in a Binding Update.

[0004] Packets for the mobile are encapsulated by the HA 16 and tunneled along tunnel 20 to the FA 18 for transmission to MN 14. In such encapsulation, an extra IP header is added to each packet, including the COA of the MN 14. This is known as FA-COA working mode.

[0005] In the second working mode (not illustrated) there is no FA, the MN 14 is allocated a unique COA and encapsulated packets are tunneled by HA 16 directly to MN 14; this is known as Collocated Care of Address mode of working (CO-COA).

[0006] In both FA-COA and CO-COA modes of working, the encapsulation generates extra headers and possibly only small payloads can be used, which results in inefficient transmission and inefficient use of expensive system and network resources, such as radio links. Further, encapsulation hides the flow identification, and the differentiation of classes of services is thus also disabled, so that Quality of Service (QoS) provision mechanisms, such as RSVP (Resource reSerVation Protocol) Int Serve, must be changed.

[0007] The disadvantages of encapsulation can be avoided by the use of Non Encapsulation Mobile IP technique, as set out in the applicant's co-pending patent application number 99301437.2 "Non-encapsulation Mobile IP" filed on 26 February 1999. In this technique, the current COA of the mobile node is used as the destination address, and the original source address, i.e., the CN address, is maintained. For FA-COA working, this deletes a header of length at least 20 bytes and introduces a header of only 2 bytes; for CO-COA mode of working no header is introduced. However a disadvantage is that any firewall or egress filtering in the home

network may reject such packets, because they have a source address different from the home network address.

[0008] It is an object of the invention to provide a method of packet addressing which overcomes the disadvantages set out above, and allows QoS to be provided.

[0009] In both the conventional encapsulation method and the two non-encapsulation techniques, the use of a home agent for redirecting packets to the current Care of Address together with the CN and MN forms so-called "triangle routing". This arrangement allows transparent inter-operation between the CN and the MN but forces all packets to be routed through the HA. One result of this is that packets may be routed along paths which are significantly longer than optimal, which can introduce delay into delivery, and also puts an unnecessary traffic load on the networks and routers involved. The technique of route optimisation is known in Mobile IP when encapsulation techniques are used, but with encapsulation, transmission of extra headers leads to lower transmission efficiency and failure of QoS differentiation.

[0010] It is a further object of the invention to provide an improved method of route optimization which avoids the disadvantage of re-directing via a HA.

[0011] According to the invention, a method of operating a third generation mobile telecommunications system, in which packets are addressed to a mobile terminal which has a correspondent node and which is currently in a foreign network, comprising the steps of setting up a home agent in the home network and allocating a Care of Address in the foreign network for the mobile terminal, characterized by the further steps of the home agent changing the packet header so that the destination address is the Care of Address, and providing a mobile node identifier, whereby route optimization is provided.

[0012] In the accompanying drawings, Figure 1 illustrates the prior art. Figure 2 illustrates the problem to be solved; and Figure 3 illustrates a prior art packet format using encapsulation technique.

[0013] The invention will be described by way of example only with reference to Figures 4 and 5 in which:-

Figure 4 illustrates a packet header format according to the invention;

Figure 5a illustrates message exchange for a RSVP session originating from a CN; and

Figure 5b illustrates a RSVP session originated in a mobile node.

[0014] In Figure 2, a mobile which is temporarily in a foreign network is shown as MN 28, which has a FA 30. The CN 24 of the mobile has set up a HA 26.

[0015] Reference to figures 1 and 2 illustrates the problem of routing all packets via HA 16 or 26 - routes may be long and will introduce delay.

[0016] Figure 3 illustrates a packet format in which an original IP packet complete with its header is encapsulated in a packet having as the source address 34, the CN 12 (see Figure 1) and as the destination address 36 the CoA of MN 14. The packet also contains other fields 38 and the payload 32 is the complete original packet.

[0017] Figure 4 shows the packet format 40 according to the invention. The source and destination addresses 44, 46 and the other fields 48 are unchanged, but the payload 42 now contains only the payload of the original packet, which gives a saving in length, but the header is lost. The packet now also contains the new field 50, the MNID, which is an identifier code for MN 28, and is only two bytes long.

[0018] The MNID field 50 is generated by FA 30, which keeps a mapping table of MNIDs and MNs. FA 30 also sends to the HA 26 the identifier for the MN 28 with which it will need to communicate to supply the mobile; conventionally the CN 24 will solicit the HA 16 for this information.

[0019] When a packet is received by FA 30, it uses the MNID information and the mapping table it holds to find for which of the several MNs it supports the packet is destined.

[0020] The MNID 50 is also used to recover the original destination address (the home address of MN 28) by replacing the MN's CoA with the MN's home IP address. When the system is operating in FACOA mode, the home IP address is found by the FA 30 looking in its mapping table of MNIDs and MNs. The FA 30 then strips the MNID field 50 from the packet, makes a correspondent adjustment of the other IP header fields, such as recalculation of the checksum, and then delivers it to the MN.

[0021] When the system is operating in COCOA mode, the MN has already received the packet; it recalculates the checksum, and delivers the packet to the higher layers of the system.

[0022] With the use of a packet in the format shown in Figure 4, the disadvantages of routing all packets via HA 26 (Figure 2) are overcome. The packets go directly to the FA 30 (FACOA working mode) or to MN 28 (COCO A working mode). Further, all necessary information for identifying the traffic flows from the correspondent node 24 to the current CoA of the mobile node 28 remains unchanged. This allows a simple adaptation of QoS session to be applied to follow the movement of the mobile as it wanders; a QoS session such as RSVP can be set up directly between CN 24 and MN 28. The class of service differentiation for QoS provision between the CN and MN will still be effective regardless of a change in the MN's network attachment point. A QoS session can have either the CN or MN as the sender. Examples will be given using RSVP (Resource Reservation Protocol) as an example.

[0023] When the CN 24 is the sender and the MN 28 is the receiver, as shown in Figure 5a, an RSVP proxy server or its equivalent in the correspondent network in-

itiates a PATH message, with the source and destination addresses being:-

CN: PATH msg: Src addr: CN  
Dest addr: MN's CoA

[0024] When the PATH message is received, either the proxy server or its equivalent in the foreign network in the MN 28 (for COCOA mode of working) or FA 30 (for FACOA mode of working) prepares a RESV message, as follows:-

MN: RESV msg: Src addr: MN's CoA  
Dest addr: CN

[0025] Other flow identification information such as protocol ID as well as source/destination port numbers are added and the message is dispatched.

[0026] In Figure 5a the FA 30 is shown dotted as it is not active in COCOA working mode.

[0027] The RESV message is routed hop-by-hop from the foreign network to the correspondent network following the same route as the PATH message but in the reverse direction. Two network switching elements or routers, 52, 54 on the routes are shown in Figure 3a. The routers change the source and address headers appropriately for each hop. When the RSVP proxy server or its equivalent in the correspondent node receives the RESV message, a RESV confirmation message is sent out, if requested, to confirm the establishment of the whole RSVP session.

[0028] When the MN 28 is the sender and the CN 24 is the receiver of a PATH message, the format is:-

MN: PATH msg: Src addr: MN's home address  
Dest addr: CN

CN: RESV msg: Src addr: CN  
Dest addr: MN's home address

[0029] The message generation and exchanges are similar to those described when the CN is the sender. However the location of the proxy server in the foreign network can now affect the message route.

[0030] If the proxy server in the foreign network is a separate entity running on a different host machine from the mobile node 28, or even built into FA 30, it will bear an IP address which is local to the foreign network but different to the MN's home address. The previous hop (PHOP) of the first routing switch or router 54 from the foreign network to the correspondent network is recorded to be the proxy server. In these circumstances, the RESV message which originated from CN 24 is successfully routed back to the foreign network and received by the proxy server.

[0031] However, if the foreign proxy server is built into the MN 28, as shown at reference 56 in Figure 5b, then the previous hop PHOP of the first routing switch 54 will

be recorded as the MN 28 at its home address. When the RESV message reaches his first hop, it will use the MN's home address as the destination address, and the RESV message will eventually be routed to the mobile node home network instead of reaching the proxy server in the foreign network.

[0032] Considering the message addressing in more detail, when MN 28 generates a PATH message, it is sent end to end to the CN, but the network sends it via the routers such as 52, 54. The first leg from proxy 56 to router 54 is addressed as:-

PATH state: previous hop: MN's home address  
next hop: R1 (52)  
from router 54 to router 52:  
PATH state: previous hop: R2  
next hop: CN (24)

[0033] When CN 24 returns a RESV message, the addressing is now hop-by-hop in the reverse direction to the PATH message, i.e., :-

RESV state: Src: CN  
Dest: R1  
from router 52 (R1) to router 54 (R2):-  
RESV state: Src R1  
Dest R2  
from router R2 (54):-  
RESV state: Src R2  
Dest MN's home address

[0034] This is indicated by the dotted arrow A in Figure 5b.

[0035] In these circumstances, the proxy server 56 in the foreign network is arranged to modify or regenerate a PATH message as follows:-

MN: PATH msg: Src addr: MN Care-of-Address  
Dest addr: CN  
CN: RESV msg: Src addr: CN  
Dest addr: MN's Care-of-Address

[0036] The PATH and RESV messages pass between the MN 28 and CN 24 as before, but now the final hop of the RESV message is correctly directed towards the MN 28 in the foreign network, as indicated by the arrow B in Figure 5b. A RESV confirmation message can also be correctly routed.

[0037] When data packets arrive at the CN 24, the MN's COA is replaced with the MN home address, which is available from the binding cache entry for the mobile node containing the mobile node home address.

[0038] Thus a QoS session can be set up successfully, no matter what the location of the proxy server.

## Claims

1. A method of operating a third generation mobile telecommunications system in which packets are addressed to a mobile node which is currently associated with a foreign network and which is communicating with a correspondent node (24), comprising the steps of setting up a home agent (26) in the correspondent node and allocating a Care of Address for the mobile terminal in the foreign network, characterized by the further steps of changing the packet header at the correspondent node so that the destination address is the Care of Address, and providing a mobile node identifier (50) whereby route optimization is provided.
2. A method according to Claim 1 in which the Care of Address represents the current location of the mobile node 28.
3. A method according to Claim 1 in which the Care of Address is the address of a foreign agent (30) in the foreign network.
4. A method according to Claim 3 in which the foreign agent (30) stores a mapping table of mobile nodes and mobile node identifiers.
5. A method according to Claim 4 in which, when a packet is received by the foreign agent (30), the foreign agent looks at its stored mapping table to locate the mobile node for which the packet is destined.
6. A method according to any preceding claim comprising the further step of providing Quality of Service for the mobile in which an end-to-end Quality of Service enquiry message is sent from the correspondent node (24) to the mobile node (28) and a Quality of Service response message is returned hop-by-hop to the correspondent node (24).
7. A method according to any one of Claims 1 to 5 comprising the further step of providing Quality of Service for the mobile in which an end-to-end Quality of Service enquiry message is sent from the mobile node (28) to the correspondent node (24), the mobile node (28) having a built-in Quality of Service proxy server (56), and the proxy server (56) changing the packet header source address to the MN Care of Address.
8. A method according to claim 6 or claim 7 in which the Quality of Service is Resource reSerVation Protocol.

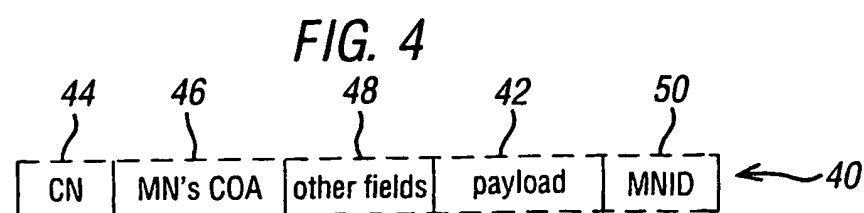
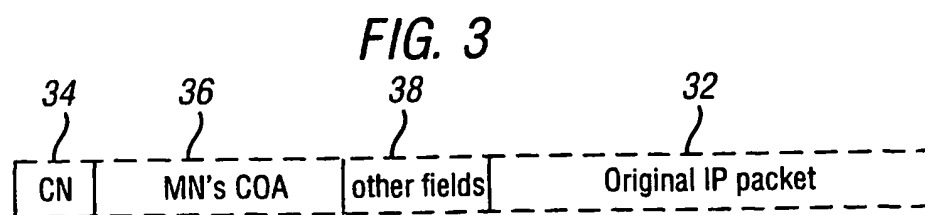
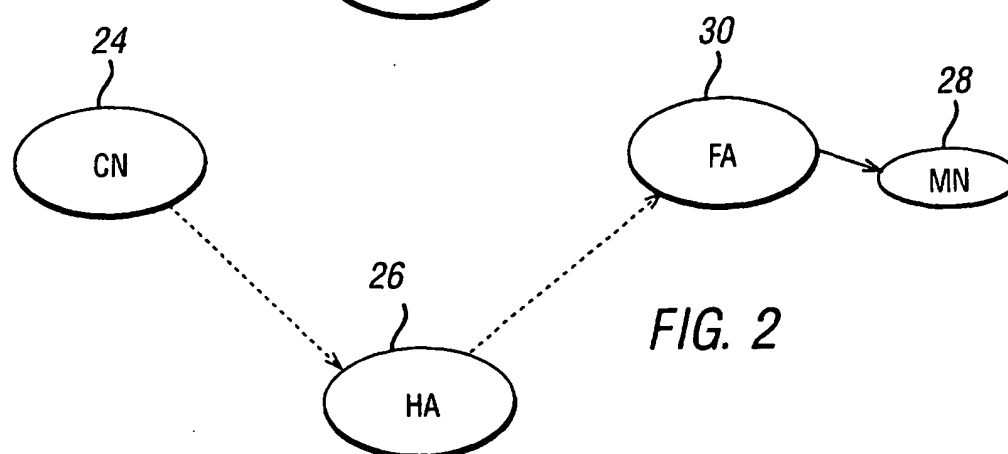
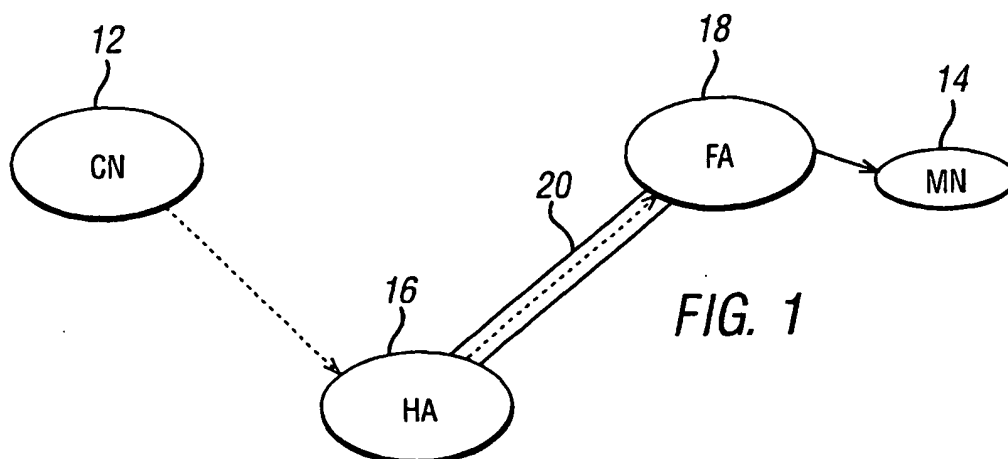


FIG. 5a

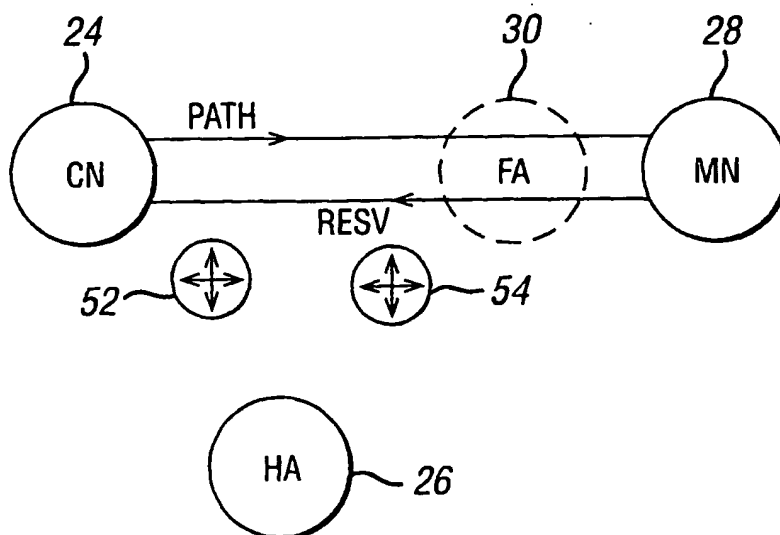


FIG. 5b

